North Dakota
Information Technology Department

ITCC

March 11,2015

ITD Room 438

Agenda

1:00	Update on EA Activity	Jeff Quast
1:15	Cloud Update	Gary Vetter
1:30	NDGOV Banner	Cliff Heyne
1:45	Privacy Standard/Template	Jeff Quast
2:00	Continued Review of ITCC Standards	Jeff Quast
2:50	Future Agenda Items	ITCC

EA Activity Update

Security Architecture

Met March 10,2015

- ITD is considering limiting access to Webmail to IP ranges in North America
  - Access outside NA would require VPN
- Continued drafting revisions to Access Control Standard – 3-5-10 failed logins for NDGOV accounts
- May combine Access Control standards and make sections for each type of platform – (NDGOV, State Login ID, Mainframe, AS400, Mobile, SaaS)

Upcoming Meetings

Application Architecture

Tuesday March 17, 2015 – 2:00 - 3:30

Data Architecture

Thursday March 19, 2015 – 10:00 - 11:30

Security Architecture

Recurring – First Tuesday – 2:00 - 3:30

Technology Architecture

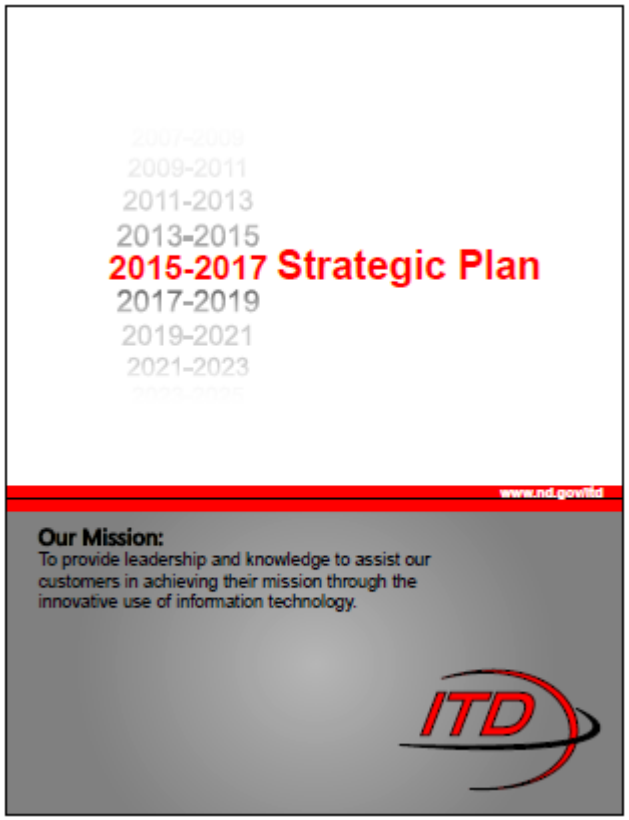
Thursday March 19, 2015 – 2:00 - 3:30

EA SharePoint

- New EA site moved to Production
  - Work in progress…feel free to experiment
  - Permissions appear to be generous…so be careful please☺
- https://wssshare.nd.gov/ea
  - Document Repository (Multiple Views)
  - Discussion Board
  - Calendar
  - Notebook (OneNote Web App)
- Next
  - Survey tool

Cloud Risk Assessment

2015-2017 Strategic Initiatives



- Develop a cloud decision-making framework

Cloud Risk Assessment

	Risk Control Area	Agency Assessment	ITD Assessment	Enterprise Tollerance
Archicture	Networking	Very low	Low	Low
	Storage	Very low	Low	Moderate
	Software	Very low	Very low	Low
	Integration	Low	Low	Moderate
	Capacity Management	Very low	Very low	Moderate
	High Availability	Low	Very low	Moderate
	IT Agility	Very low	Very low	Very low
	Portability	Very low	Very low	Very low
	Service Termination	Very low	Very low	Low
Security	Data Center Operations	Low	Low	Low
	Identity	Low	Moderate	Low
	Audit and Compliance	Very low	Very low	Low
	Logging and Tracing	Very low	Low	Very low
	Malicious Activities from Within	Low	Low	Low
Data	Data Classification	Low	Low	Moderate
	Data Migration	Low	Low	Low
	Data backup	Very low	Very low	Moderate
	Data Sanitization	Very low	Low	Moderate
	Records Management	Very low	Low	Low
	Electronic Discovery	Very low	Low	Moderate
Strategy	Mission Criticality	Low	Low	Low
	User Expectations	Low	Low	Low
	Customer-facing Implications	Low	Low	Low
	Availability	Low	Low	Low
	Provider Selection	Low	High	Low
	Organizational Readiness	Low	Low	Very low
	Incident Management	Low	Low	Very low
	Ongoing Maintenance	Low	Low	Very low
	IT Skillsets	Low	Low	Very low
	Disaster Recovery	High	Low	Very low
	Finance	Very low	Low	Very low
	3rd-Party Involvement	Very low	Low	Low

Risk Control Areas

- Architecture
- Security
- Data
- Strategy

Perspectives

- Agency Assessment
- ITD Assessment
- Enterprise Tolerance

Cloud Risk Assessment

	Risk Control Area	Agency Assessment	ITD Assessment	Enterprise Tollerance
Archicture	Networking	Very low	Low	Low
	Storage	Very low	Low	Moderate
	Software	Very low	Very low	Low
	Integration	Low	Low	Moderate
	Capacity Management	Very low	Very low	Moderate
	High Availability	Low	Very low	Moderate
	IT Agility	Very low	Very low	Very low
	Portability	Very low	Very low	Very low
	Service Termination	Very low	Very low	Low
Security	Data Center Operations	Low	Low	Low
	Identity	Low	Moderate	Low
	Audit and Compliance	Very low	Very low	Low
	Logging and Tracing	Very low	Low	Very low
	Malicious Activities from Within	Low	Low	Low
Data	Data Classification	Low	Low	Moderate
	Data Migration	Low	Low	Low
	Data backup	Very low	Very low	Moderate
	Data Sanitization	Very low	Low	Moderate
	Records Management	Very low	Low	Low
	Electronic Discovery	Very low	Low	Moderate
Strategy	Mission Criticality	Low	Low	Low
	User Expectations	Low	Low	Low
	Customer-facing Implications	Low	Low	Low
	Availability	Low	Low	Low
	Provider Selection	Low	High	Low
	Organizational Readiness	Low	Low	Very low
	Incident Management	Low	Low	Very low
	Ongoing Maintenance	Low	Low	Very low
	IT Skillsets	Low	Low	Very low
	Disaster Recovery	High	Low	Very low
	Finance	Very low	Low	Very low
	3rd-Party Involvement	Very low	Low	Low

Risk Likelihood

- Slight
- Not likely
- Likely
- Highly likely
- Expected

Risk Impact

- Low
- Mild
- Serious
- Severe
- Catastrophic

Cloud Risk Assessment

Architecture	Networking	Insufficient controls and/or incompatible architecture to securely provide network connectivity/capacity
	Storage	Insufficient controls and/or incompatible architecture to securely store data
	Software	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Integration	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Capacity Management	Unable to proactively load-test, monitor (by State), and/or scale application performance
	High Availability	Insufficient architecture to provide geographically distributed high-availability
	IT Agility	Latency or overall difficulty in implementing/adjusting system architecture to address technical and/or business requirements
	Portability	Technical and/or non-technical dependencies create vendor lock-in and/or limit future options for migrating service elsewhere
	Service Termination	Insufficient control/confidence with regard to either party terminating service and the State's ability to transfer functionality elsewhere

Cloud Risk Assessment

Security	Data Center Operations	Insufficient controls/testing of data center redundancy/security
	Identity	Insufficient controls and/or incompatible architecture to provide proper identity and access management
	Audit and Compliance	Insufficient controls in place to properly measure and meet regulatory requirements/certifications
	Logging and Tracing	Insufficient controls and/or access to properly manage operational logs for troubleshooting and regulatory compliance
	Malicious Activities from Within	Insufficient control/confidence with regard to privileged users performing unauthorized/unlawful activities such as data theft, tampering, leakage, etc.

Data	Data Classification	Unclear classification of data and/or insufficient control/confidence with regard to safeguarding sensitive/confidential data
	Data Migration	Difficulty in moving legacy data into a new environment
	Data backup	Insufficient backup/recovery procedures, lack of geographical separation of media, and/or misplacement or theft of backup information
	Data Sanitization	Insufficient control/confidence with regard to properly identifying and physically destroying sensitive media
	Records Management	Insufficient control/confidence with regard to data being stored, retained, and purged to a compliant level
	Electronic Discovery	Insufficient access to data upon request and/or insufficient control with regard to subpoenas, jurisdiction, and confiscation of data

Cloud Risk Assessment

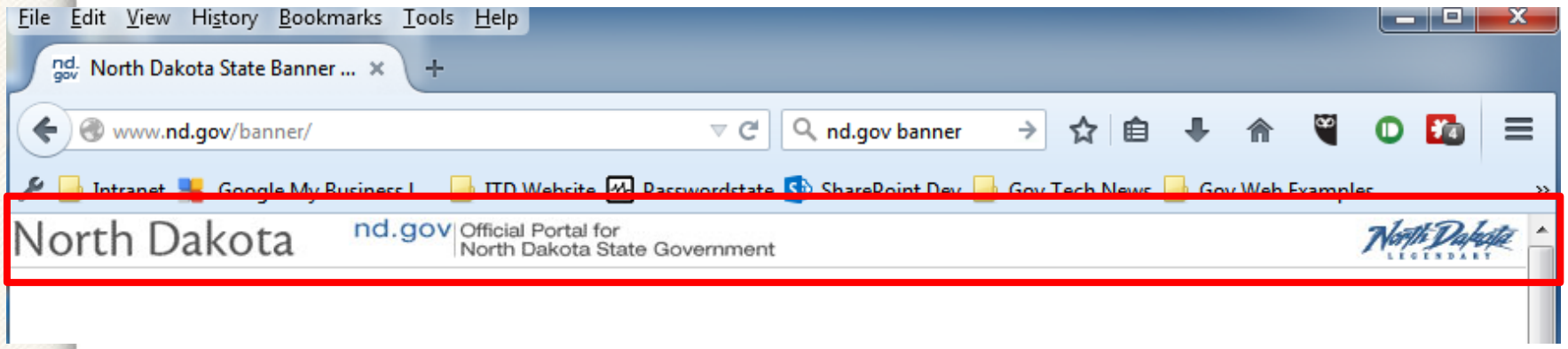
Strategy	Mission Criticality	Unable to provide critical government services if the provider experiences a loss of service
	User Expectations	Inability to fulfill user expectations, especially with regard to performance and/or ease-of-use
	Customer-facing Implications	Unable to maintain a positive stakeholder perception and/or State reputation
	Availability	Insufficient uptime guarantees and/or reliability
	Provider Selection	Insufficient confidence with regard to the provider's completeness of vision and ability to execute; in the past, present, and future
	Organizational Readiness	Insufficient preparation with regard to strategic alignment, workforce readiness, cultural impact, and/or stakeholder buy-in
	Incident Management	Insufficient controls in place detect, report, and resolve disruptions in service
	Ongoing Maintenance	Insufficient control over the process, frequency, scheduling, and functionality of maintenance/enhancements
	IT Skillsets	Insufficient IT resources/training to properly implement/manage the application and/or an unclear shift in IT roles/responsibilities
	Disaster Recovery	Insufficient control/capability/confidence with regard to handling natural disasters and maintaining business continuity
	Finance	Insufficient preparation within accounting/budgeting procedures to shift from capital to operational expenditures
	3rd-Party Involvement	Insufficient control and/or over-dependency upon 3rd party hosting providers

SMUG Agenda

March 12, 2015 – ITD Rm 438

1. Introduction (5 min)
2. Social media management tools presentation (25 min)
3. Managing agency social media accounts (15 min)
4. ND.gov privacy policy (10 min)
5. ND.gov website banner (10 min)
6. Expanded agency resources (10 min)
7. Open discussion (15 min)

ND.GOV BANNER



OLD

North Dakota
LEGENDARY

NEW

North Dakota®
LEGENDARY

http://www.nd.gov/banner

Digital Communication in state government

Review of ITCC Standards

- Copyright and Trademarks Guideline
- E-Services Privacy
- E-Services Privacy Policy Best Practices
- Web Domain Name Best Practices
- Web Domain Name Standard